

# On the existence of quantum signature for quantum messages

Qin Li<sup>a,b,\*</sup>, Wai Hong Chan<sup>c</sup>, Chunhui Wu<sup>d</sup>, Zhonghua Wen<sup>a</sup>

<sup>a</sup>College of Information Engineering, Xiangtan University, Xiangtan 411105, China

<sup>b</sup>Key Laboratory of Intelligent Computing and Information Processing of the Ministry of Education, Xiangtan University

<sup>c</sup>Department of Mathematics and Information Technology, The Hong Kong Institute of Education, Hong Kong

<sup>d</sup>Department of Computer Science, Guangdong University of Finance, Guangzhou 510521, China

---

## Abstract

Quantum signature (QS) is used to authenticate the identity of the originator, ensure data integrity and provide non-repudiation service with unconditional security using quantum theories. It can be generally considered as arbitrated QS if a trusted third party named arbitrator is involved, and true QS if otherwise. In this paper, we shall analyze why arbitrated QS is possible to sign quantum messages by providing a basic framework, and settle the disagreements between the impossibility of true QS [1] and an existing true QS scheme for quantum messages [2].

*Keywords:* Quantum cryptography, Quantum signature, Existence Analysis

---

## 1. Introduction

Digital signature, as an analogy to hand-written signature for authenticating the origin of a message and ensuring the message not being modified during transmission, is an essential cryptographic primitive. It has been being widely used in various fields, particularly in secure electronic commerce. As Rivest predicted, digital signature may become one of the most fundamental and useful inventions of modern cryptography [3]. However, all of the existing classical (digital) signature schemes whose security depends on the difficulty of solving some hard mathematical problems were threatened by last-increasing power of computers and innovative techniques such as quantum computation. For instance, once quantum computers would be successfully built, most of classical signature schemes would be cracked through Shor's algorithm [4]. On the other hand, quantum physics has thrown light on the study of cryptography for obtaining unconditional security [5, 6, 7, 8, 9, 10]. Therefore, researchers turn to investigate quantum counterpart of classical signature with the hope that quantum signature (QS) can provide unconditional security which ensures that the attacker (or the malicious receiver) cannot forge the signature, and, in the same time, the signatory cannot deny the signature even though unlimited computing resources are available.

QS is expected to sign both classical and quantum messages, and the form of each quantum message can be a known or an unknown quantum state. Since known quantum states can be characterized with classical information, the quantum messages being considered in this paper are in the form of unknown quantum states. Over the last decade, researchers have made some progress on QS. In 2001, Gottesman and Chuang proposed a QS scheme based on quantum one-way function, which is unconditionally secure even against quantum attacks [11]. However, this scheme works only on classical messages, and seems not practicable as it would use up  $O(m)$  qubits of the public key for signing an  $m$ -bit message. What is even worse happened in 2002, Barnum *et al.* showed that unconditionally secure QS for quantum messages is impossible [1]. This no-go theorem really disappointed many quantum cryptography researchers, but it did not abort the study of QS. In the same year, Zeng and Keitel presented a QS scheme which can sign both classical and

---

\*Corresponding author.

Email address: liqin@xtu.edu.cn (Qin Li)

quantum messages by introducing a trust third party named arbitrator [12] and the scheme was improved later [13, 14]. Afterwards, Li *et al.* observed that the GHZ states used in [14] could be replaced with Bell states. They then put forward a more efficient scheme in [15]. Not long after that, Zou *et al.* showed both the two schemes proposed in [14] and [15] are insecure since they could be repudiated by the receiver Bob, and further presented two arbitrated QS schemes to fix the problem [16]. Some other arbitrated QS schemes were also proposed since the study of arbitrated QS was initiated by Zeng and Keitel [17, 18, 19, 20, 21].

However, most typical arbitrated QS schemes were cryptanalyzed recently [22, 23, 24, 25, 26]. Some researchers begin to doubt whether unconditionally secure arbitrated QS schemes for quantum messages are really possible to exist. In order to allay doubts in this regard, we shall give a detailed analysis in this paper for explaining the reasons why the existence of arbitrated QS does not contradict Barnum *et al.*'s conclusion, although some of those reasons were preliminarily mentioned by Li *et al.* in [15]. We will also show that unconditionally secure arbitrated QS for quantum messages is possible. In addition, Zeng *et al.* presented a true QS scheme in 2007 and claimed it can sign quantum messages with unconditional security [2]. This result excited the nerves of researchers in the field, and people asked: Is Barnum *et al.*'s conclusion [1] wrong or Zeng *et al.*'s scheme [2] insecure? We shall provide the answer by showing the insecurity of Zeng *et al.*'s scheme.

The rest of the paper is arranged as follows. Sec. 2 briefly reviews Barnum *et al.*'s no-go theorem for signing quantum messages. Then we show the arbitrated QS can be used to sign quantum messages in Sec. 3, and solve the disagreements between the impossibility of true QS and an existing true QS scheme for quantum messages in Sec. 4. The last section concludes the paper.

## 2. Review of the no-go theorem for signing quantum messages

This section briefly reviews Barnum *et al.*'s no-go theorem [1], saying that signing quantum messages is impossible to realize.

Barnum *et al.* gave a detailed proof of the theorem which they offered in [1] that quantum authentication implies encryption. In other words, any scheme which wants to ensure the authenticity of quantum messages must also encrypt them almost perfectly. However, in a QS scheme, the receiver should learn something about the contents of the quantum message but is not allowed to change it. It follows that the theorem results the impossibility of signing quantum messages since any non-trivial information gain from encrypted quantum messages is only possible at the cost of introducing disturbance to them which destroys the authenticity of quantum messages.

To be more intuitive, one can assume the receiver is allowed to efficiently extract the original quantum message  $\rho$ , then it is easy to show the receiver can generate a valid signature of a new message  $\rho'$  favorable to him by the following steps. First suppose the receiver can extract the original message  $\rho$  via the transformation  $U$  and leave the auxiliary state as  $\varphi$  which may not be held entirely by the receiver. Since  $\rho$  should have been entangled with a reference system,  $\varphi$  must be independent of  $\rho$ . Then the receiver implements the transformation  $U^\dagger$ , which is the inverse process of  $U$ , on  $\rho'$  and his part of  $\varphi$  to get a valid signature. Obviously, this contradicts the security of the QS scheme and thus signing quantum messages is impossible.

## 3. Possibility of arbitrated QS for quantum messages

In this section, we analyze why using arbitrated QS to sign quantum messages does not disagree with Barnum *et al.*'s conclusion [1], and explain why it is possible to provide unconditional security by giving a basic framework of such a scheme.

Although almost all existing arbitrated QS schemes were cracked recently [22, 23, 24, 25, 26], it does not mean that arbitrated QS cannot provide unconditional security. The failures of the previous schemes are mainly due to imperfections of their design. For example, all those schemes just employed quantum one-time pad to encrypt, but ignored, to authenticate the transmitted quantum messages. Quantum encryption does not imply authentication, even though the converse is true [1]. Thus, the malicious receiver can change the signed quantum message and the corresponding signature without being detected by implementing appropriate unitary operations.

According to Barnum *et al.*'s no-go theorem, signing quantum messages is impossible because any protocol which allows one receiver to read a quantum message also allows the receiver to modify the message without the risk of being detected, and therefore all potential receivers of an authenticated message must be trustworthy. In any arbitrated QS scheme, the arbitrator is always supposed to be trusted by both signatory and receiver; we can assume that the real recipient of the authenticated message is the arbitrator who is in charge of the verification of the signature. After verifying the signature, the arbitrator can send a parameter to indicate whether the signature is valid. The receiver would obtain the indication parameter, and only need to check whether the parameter and other information come from the real arbitrator. Based on this idea, we can give a basic framework of an unconditionally secure arbitrated QS scheme for quantum messages.

For better understanding, we introduce two denotations before presenting the scheme.  $Aut_K(\cdot)$  denotes that unconditionally secure authentication with the key  $K$  is used such as the quantum authentication scheme given in [1] for quantum information, and Wegman-Carter authentication scheme for classical information in [27].  $Sig_K(\cdot)$  is an abstract secret transformation in terms of the key  $K$ . In an arbitrated QS scheme, there are generally three phases: the initial phase, the signing phase, and the verification phase as shown below:

- (1) At first, the signatory Alice shares a key  $K_{Aa}$  with the arbitrator and the receiver Bob also has a key  $K_{Ba}$  shared with the arbitrator. This step constitutes the initial phase.
- (2) Alice generates the signature  $Sig_{SK_A}(P)$  of the message  $P$  and computes  $\sigma = Aut_{K_{Aa}}(Sig_{SK_A}(P), P)$  for authentication. Note that being the signing key of Alice,  $SK_A$  is always private. Alice then sends the authenticated signature state  $\sigma$  to Bob. This is the signing phase.
- (3) In the beginning of the verification phase, Bob produces  $Y = Aut_{K_{Ba}}(\sigma)$  and transmits it to the arbitrator.
- (4) The arbitrator checks the authenticity of  $\sigma$  with the key  $K_{Ba}$ . If there is anything wrong, the arbitrator would abort the protocol immediately; otherwise, the arbitrator would examine whether  $Sig_{SK_A}(P)$  and  $P$  are tampered or not. If not, the arbitrator would verify whether  $Sig_{SK_A}(P)$  is a valid signature by employing some secret information such as that related to Alice's signing key and public information  $PK_A$  which is known to the arbitrator or receivers. If the verification process is passed, the arbitrator sets the verification parameter,  $r = 1$ ; or else,  $r = 0$ . Finally, the arbitrator computes  $T = Aut_{K_{Ba}}(P, Sig_{SK_A}(P), r)$  and sends it to Bob.
- (5) Bob authenticates what he have received. If the authentication test is passed and  $r = 1$ , he would accept  $Sig_{SK_A}(P)$  as the signature of  $P$ . This finishes the whole verification process.

Although the above arbitrated QS scheme is trivial, it obviously can avoid the attacks proposed recently in [22, 23, 24, 25, 26] due to the use of authentication. In addition, under our assumption that the arbitrator is trustworthy and is the only person who can verify  $Sig_{SK_A}(P)$  with all the information he holds, the proposed scheme is not only unconditionally secure, but also adaptive to Barnum *et al.*'s conclusion. Actually, even if Bob can directly verify  $Sig_{SK_A}(P)$  only with  $PK_A$  and produce the signature  $Sig_{SK_A}(P')$  of another message  $P'$  favorable to him using the method given by Barnum *et al.*, he is still not able to generate  $\sigma' = Aut_{K_{Aa}}(Sig_{SK_A}(P'), P')$  without knowing the key  $K_{Aa}$ . Hence he would not be able to convince other receivers that  $(P', Sig_{SK_A}(P'))$  is a valid message-signature pair. This tells that the verification made by the arbitrator is indispensable to an arbitrated QS scheme.

#### 4. Settlement of Conflicts

We begin with reviewing Zeng *et al.*'s true QS scheme which was claimed to be able to sign quantum messages with unconditional security [2]. Then we show the insecurity of the scheme by attacking it successfully using similar method presented by Barnum *et al.* in [1].

#### 4.1. Review of the existing true QS scheme

Zeng *et al.* proposed a true QS scheme for the purpose of signing quantum messages based on a suitable one-way function recently [2] and claimed that the scheme is unconditionally secure. We briefly describe the three phases (initial, signing and verification) of their scheme in the following. More details can be found in [2].

- In the initial phase, the main goal is to generate the signature key  $K_s$  and the verification key  $K_v$  by constructing a one-way transformation  $G : \{L, X, T_{ij}\} \rightarrow \{U, \|T\|^{1/2}\}$ , where  $L$  is a linear transformation mapping  $x = (x_0, x_1, \dots, x_{k-1}) \in \mathbb{R}^k$  to  $y(X) = y_0(x) = [x_0, y_1(x), \dots, y_{2k-1}(x)]^T \in \mathbb{R}^{2k}$  and making any  $k$ -element subset of  $\{x_0, y_1, \dots, y_{2k-1}\}$  linearly independent,  $T$  satisfies  $T[y_{r_1}, y_{r_2}, \dots, y_{r_k}]^T = T[x_0, y_{r_{k+1}}, \dots, y_{r_{2k-1}}]^T$ , and  $U$  makes  $U|y_{r_1}\rangle_{r_1}|y_{r_2}\rangle_{r_2}\dots|y_{r_k}\rangle_{r_k} = |x_0\rangle_{r_1}|y_{r_{k+1}}\rangle_{r_2}\dots|y_{r_{2k-1}}\rangle_{r_k}$ .  $K_s$  is expressed as  $K_s = \{L, X\}$  and  $K_v$  is set as  $K_v = \{U, \|T\|^{1/2}\}$ .
- In the signing phase, according to  $K_s$ , the signatory Alice prepares  $2k - 1$  ancilla states  $|\omega(X)\rangle = |y_1(X)\rangle_1 \dots |y_{2k-1}(X)\rangle_{2k-1}$  and encodes the message state  $P$  with a wave function  $\langle x_0|P\rangle$  as  $|\tilde{S}\rangle = \int |P\rangle|\omega\rangle dX$ . Then Alice prepares a two-particle entangled state  $|\tilde{\Omega}\rangle = \int_{\mathbb{R}} |y_{k+1}\rangle_{r_2}|y_{k+1}\rangle_{r_{k+1}} dx$  in terms of  $K_s$  and generates a signature state  $|S\rangle = |\tilde{S}\rangle \otimes |\tilde{\Omega}\rangle$ . Finally  $|S\rangle$  and  $|P\rangle$  are sent to the receiver Bob.
- Bob implements the verification process by the following four steps: (1) Bob checks whether the state  $|S\rangle$  is a  $2k$ -particle QECC by performing a syndrome measurement on it. (2) In terms of  $K_v$ , Bob decodes  $|S\rangle$  as

$$\begin{aligned} K_v|S\rangle &\rightarrow U|\tilde{S}\rangle \\ &= J\|T\|^{1/2} \int \{|P\rangle_{r_1}|y_{r_{k+1}}\rangle_{r_2}|y_{r_{k+1}}\rangle_{r_{k+1}}\dots \\ &\quad \otimes |y_{r_{2k-1}}\rangle_{r_k}|y_{r_{2k-1}}\rangle_{r_{2k-1}}\} dX \\ &= J\|T\|^{1/2} |P\rangle_{r_1} |\Omega\rangle_{r_2, r_{k+1}} |\Omega\rangle_{r_3, r_{k+2}} \dots |\Omega\rangle_{r_k, r_{2k-1}}, \end{aligned} \tag{1}$$

where  $J$  is the Jacobian for the transformation from  $X$  to  $y(X)$ , and  $|\Omega\rangle_{i,j} = \int_{\mathbb{R}} |y_l\rangle_i |y_l\rangle_j dx (i = r_2, \dots, r_k, j, l = r_{k+1}, \dots, r_{2k-1})$ , which is an entanglement state of particles  $i$  and  $j$ . (3) Bob verifies the entanglement properties of  $k - 1$  states  $|\Omega\rangle_{r_2, r_{k+1}}, |\Omega\rangle_{r_3, r_{k+2}}, \dots, |\Omega\rangle_{r_k, r_{2k-1}}$ , respectively. (4) Bob checks whether the decoded message state is the same as the received message state, and tests the equality of the decoded two-particle entangled state  $|\Omega\rangle_{r_2, r_{k+1}}$  and the received two-particle entangled state  $|\tilde{\Omega}\rangle$ . If there is a failure in any step, Bob will reject  $|S\rangle$  and stop the protocol.

#### 4.2. Insecurity of the existing true QS scheme

The above scheme used for signing quantum messages [2] does not involve a trustable arbitrator to help the receiver verify the signature. Any receiver who is not always trustworthy can verify the validity of the signature directly. This scheme obviously violates Barnum *et al.*'s conclusion [1] which stated that signing quantum messages is impossible since any scheme which allows one receiver to read a quantum message also allows the receiver to modify the message without the risk of being detected, and therefore all potential receivers of an authenticated message must be trustworthy. Therefore, if Barnum *et al.*'s conclusion is right, Zeng *et al.*'s scheme cannot be secure; or the other way round. In the following, we show that Barnum *et al.*'s conclusion also adapts to Zeng *et al.*'s scheme and the scheme is insecure.

Firstly, we assume the receiver Bob gets the message  $P$  and the corresponding valid signature  $|S\rangle = |\tilde{S}\rangle \otimes |\tilde{\Omega}\rangle$  using Zeng *et al.*'s scheme. We then show Bob can forge a valid signature  $|S'\rangle$  of another message  $P'$  beneficial to him using the following steps: 1) After decoding the state  $|\tilde{S}\rangle$  using the way expressed in Eq. (1), Bob replaces the decoded message state  $|P\rangle$  with a new message state  $|P'\rangle$ , and the state of the whole system is changed to  $|\Phi\rangle = J\|T\|^{1/2} |P'\rangle_{r_1} |\Omega\rangle_{r_2, r_{k+1}} |\Omega\rangle_{r_3, r_{k+2}} \dots |\Omega\rangle_{r_k, r_{2k-1}}$ . 2) Bob applies  $U^\dagger$  which is the inverse transformation of  $U$  on  $|\Phi\rangle$  to get  $|\tilde{S}'\rangle = U^\dagger|\Phi\rangle$ . 3) Bob generates the signature state  $|S'\rangle = |\tilde{S}'\rangle \otimes |\tilde{\Omega}\rangle$

of  $|P'\rangle$  by combining  $|\tilde{S}'\rangle$  and  $|\tilde{\Omega}\rangle$ . The new message-signature pair  $(P', |S'\rangle)$  is valid since it can be shown to pass the four steps of the verification phase: since  $|S\rangle$  which Bob holds is a valid signature, the entanglement properties of  $|\Omega\rangle_{r_2, r_{k+1}}, |\Omega\rangle_{r_3, r_{k+2}}, \dots, |\Omega\rangle_{r_k, r_{2k-1}}$  are kept and the decoded state  $|\Omega\rangle_{r_2, r_{k+1}}$  will be the same as  $|\tilde{\Omega}\rangle$ ; hence Step (3) and Step (4) can be passed. Moreover, due to  $U|\tilde{S}'\rangle = UU^\dagger|\Phi\rangle = |\Phi\rangle$ , Step (2) should also be passed. Finally, suppose  $|S''\rangle = |\tilde{S}''\rangle \otimes |\tilde{\Omega}\rangle$  is the correct signature of  $|P'\rangle$ .  $|\tilde{S}''\rangle$  must be a  $2k$ -particle QECC. As  $U|\tilde{S}''\rangle = |\Phi\rangle = U|\tilde{S}'\rangle$ ,  $|\tilde{S}'\rangle$  is identical to  $|\tilde{S}''\rangle$  and also is a  $2k$ -particle QECC which implies that Step (1) will be passed.

## 5. Conclusion

In this paper, we have shown arbitrated QS does not disobey Barnum *et al.*'s conclusion about the impossibility of QS for quantum messages [1], and have proven that it is possible to sign quantum messages with unconditional security by given a basic framework of such a scheme. In addition, we have also explained that the existing true QS scheme presented by Zeng *et al.* [2] cannot get rid of the restriction of Barnum *et al.*'s no-go theorem because the scheme is insecure. But still, Barnum *et al.*'s conclusion does not preclude the possibility of QS for classical messages. So, how to construct efficient QS schemes to sign classical messages will be the direction of our work in the near future.

## Acknowledgement

This work is partially supported by Natural Science Foundation of China (Grant Nos. 61202398, 61272295, and 61070232), Scientific Research Fund of Hunan Provincial Education Department (Grant No. 12C0400), Internal Research Grant of The Hong Kong Institute of Education (Grant No. RG 66/11-12), and the Foundation for Distinguished Young Talents in Higher Education of Guangdong (Grant No. LYM11093).

## References

- [1] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, A. Tapp, Authentication of quantum messages, in: Proceedings of the 43th Annual IEEE Symposium on Foundations of Computer Science, 2002, pp. 449–458.
- [2] G. H. Zeng, M. Lee, Y. Guo, G. Q. He, Continuous variable quantum signature algorithm, International Journal of Quantum Information 5 (2007) 553–573.
- [3] R. Rivest, Cryptography, Vol. 1, Elsevier, 1990, Ch. 13, pp. 715–755, handbook of Theoretical Computer Science.
- [4] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in: Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, 1994, pp. 124–134.
- [5] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 1984, pp. 175–179.
- [6] A. K. Ekert, Quantum cryptography based on bell's theorem, Physical Review Letters 67 (1991) 661–663.
- [7] G. Brassard, The dawn of a new era for quantum cryptography: The experimental prototype is working!, Sigact News 20 (1989) 78–82.
- [8] H.-K. Lo, H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science 283 (1999) 2050–2057.
- [9] C. H. Bennett, D. P. Divincenzo, Quantum information and computation, Nature 404 (2000) 247–255.
- [10] D. Mayers, Unconditional security in quantum cryptography, Journal of the ACM 48 (2001) 351–406.
- [11] D. Gottesman, I. L. Chuang, Quantum digital signatures, arXiv:quant-ph/0105032 (2001).
- [12] G. H. Zeng, C. H. Keitel, Arbitrated quantum-signature scheme, Physical Review A 65 (2002) article no. 042312.
- [13] M. Curty, N. Lütkenhaus, Comment on “arbitrated quantum-signature scheme”, Physical Review A 77 (2008) article no. 046301.
- [14] G. H. Zeng, Reply to “comment on ‘arbitrated quantum-signature scheme’”, Physical Review A 78 (2008) article no. 016301.
- [15] Q. Li, W. H. Chan, D. Y. Long, Arbitrated quantum signature scheme using bell states, Physical Review A 79 (2009) article no. 054307.
- [16] X. F. Zou, D. W. Qiu, Security analysis and improvements of arbitrated quantum signature schemes, Physical Review A 82 (2010) article no. 042325.
- [17] H. Lee, C. Hong, C. Kim, J. Lim, H. J. Yang, Arbitrated quantum signature scheme with message recovery, Physics Letters A 321 (2004) 295–300.

- [18] X. Lü, D. G. Feng, An arbitrated quantum message signature scheme, in: Proceedings of the 1st International Symposium on Computational and Information Science, 2004, pp. 1054–1060.
- [19] X. Lü, D. G. Feng, Quantum digital signature based on quantum one-way functions, in: Proceedings of the 7th International Conference on Advanced Communication Technology, 2005, pp. 514–517.
- [20] J. Wang, Q. Zhang, C. J. Tang, Quantum signature scheme with message recovery, in: Proceedings of the 8th International Conference on Advanced Communication Technology, 2006, pp. 1375–1378.
- [21] J. Wang, Q. Zhang, C. J. Tang, Efficient quantum signature protocol of classical messages, Journal on Communications 28 (2007) 64–68, in Chinese.
- [22] F. Gao, S. J. Qin, F. Z. Guo, Q. Y. Wen, Cryptanalysis of the arbitrated quantum signature protocols, Physical Review A 84 (2011) article no. 022344.
- [23] J. W. Choi, K. Y. Chang, D. Hong, Security problem on arbitrated quantum signature schemes, Physical Review A 84 (2011) article no. 062330.
- [24] Z. W. Sun, R. G. Du, B. H. Wang, D. Y. Long, Improving the security of arbitrated quantum signature protocols, available at arXiv:quant-ph/1107.2459 (2011).
- [25] S.-K. Chong, Y.-P. Luo, T. Hwang, On the “security analysis and improvements of arbitrated quantum signature schemes”, available at arXiv:quant-ph/1105.1232 (2011).
- [26] T. Hwang, Y.-P. Luo, S.-K. Chong, Comment on “security analysis and improvements of arbitrated quantum signature”, available at arXiv:quant-ph/1109.1744 (2011).
- [27] M. N. Wegman, L. Carter, New hash functions and their use in authentication and set equality, Journal of Computer and System Sciences 22 (1981) 265–279.